ABSTRACT OF THE DISCLOSURE

A mechanism for securely decompiling representations of objects into copies of the objects is described. A virtual machine (e.g. the Java Virtual Machine (JVM)) may include extensions for decompiling data representation language (e.g. XML) representations of objects into objects. The decompiler API may accept a data stream, which includes a representation of the object, and output a copy of the object. In one embodiment, during the decompilation of the representation of objects, each message may be checked to verify that the user has access rights to the object. Access right information for the object may be embedded in the message(s) containing the representation of the object. In one embodiment, when the user is done using the client, the user may log off or otherwise signal the user is finished with the client. In one embodiment, the user may have a "smart card" or other physical device to gain access to the client. The user may insert the smart card into the client device to begin the session. When the client is finished, the client may remove the smart card. The client may detect the removal of the smart card, and thus detect that the client is finished, and may then proceed to delete objects created by decompilation of representations. In another embodiment, at least some of the objects created on the client persistently may be stored for later access by the user or other authorized users.